A Probabilistic Approach towards the Prevention of Error Propagation Effect of AES and Realization Thereof

B. Sarkar[1], C. T. Bhunia[2], U. Maulik[3]
[1]Dr. B. C. Roy Engineering College, Durgapur, India
E-mail: sarkar.bikramjit@gmail.com
[2]National Institute of Technology, Arunachal Pradesh, India & International Centre for Theoretical Physics, Italy.
E-mail: directornitap@gmail.com,
[3]Jadavpur University, Kolkata, India
E-mail: ujjwal_maulik@yahoo.com

***Abstract*–Error propagation effect of Advanced Encryption Standard (AES) is a great research challenge. AES suffers from a major limitation of Error propagation effect. In literature, several studies have been made on this issue and several techniques are suggested to tackle the effect. To tackle this limitation, two methods are available. One is Redundancy Based Technique and the other one is Bite Based Parity Technique. The first one has a significant advantage of correcting any error on definite term over the second one but at the cost of higher level of overhead and hence lowering the processing speed. In this paper we have proposed a probabilistic technique to combat the Error Propagation Effect, which definitely guarantees a secured communication.**

***Index Terms*–AES, encryption, decryption, bit error, error propagation, majority rule, secured communication.**

I. Introduction

DES (Data Encryption Standard) was the sole authority of the Symmetric encryption schemes. Due to several recent past reports of failure [1, 2] of security or key of DES, AES (Advance Encryption Standard) has been developed as a supplement of DES. The supplement has aimed to provide higher level of security mainly with higher key size. Besides the higher level of security, AES has aimed to provide higher efficiency and better flexibility by means of encryption at different levels and with different block sizes [3]. But AES suffers from a major limitation of error propagation in the encryption process. The AES encryption is done at several rounds of iteration. Each round of iteration has different input data and different keys. The input data and the keys of different round are all generated from the original source data and the source key respectively. Thus the input data and the keys at rounds follow a data path and key path respectively. Any bit error(s) at any round, if occurs either at the data path or at the key path, results in the propagation of the error leading to the generation of huge errors at the output cipher.

The research [4, 5] reported this limitation of AES in their authoritative work. In the thesis work we have proposed a probabilistic approach for the prevention of the Error Propagation Effect of AES, which definitely guarantees a secured communication.

II. Proposed Scheme

We get the cipher text from the plain text after the AES encryption of 10 rounds. Here we consider that both the block size (plain text) and the key size are of 128 bits.

The proposed scheme suggests that first the plain text should be encrypted odd number of times, say n, with the same key. As a consequence, n number of cipher text would be generated. Now it is assumed that the probability of occurrence of a single bit error amidst the rounds must not reach 0.5 so that out of n cipher texts at most (n – 1)/2 number of cipher texts may be erroneous whereas the least number of error free cipher texts is (n + 1)/2 out of n. After getting n cipher texts, Majority Rule is applied over them and as a result the error free cipher text is achieved and is to transmit to the secured channel. It should be noted that since the number of error free cipher texts is higher than that of the erroneous ciphers, the Majority Rule applied will always culminate in the generation of the error free cipher. The proposed scheme would be made more transparent through a suitable block diagram shown in Figure 1.

Proposed Algorithm: SBM 1.2

1. Input the plain text (original message) P of 128 bits.
2. Encrypt the plain text n number of times with AES Encryptor to find ciphers $\{C_i, i = 1 \text{ to } n\}$, n being odd.
3. Majority rule is applied over C_i to find the error-free cipher text C which may directly be transmitted through the channel.

III. Experimental Result

We have conducted the experiment with the following 128-bit plain text:

B i k r a m j i t S a r k a r

Below are the corresponding Hexadecimal values:

42 69 6B 72 61 6D 6A 69 74 20 53 61 72 6B 61 72

The message (plain text) is encrypted through a 128-bit Cipher key having the corresponding Hex values as follows:

2B 28 AB 09 7E AE F7 CF 15 D2 15 4F 16 A6 88 3C

DOI: 01.IJNS.3.4.2

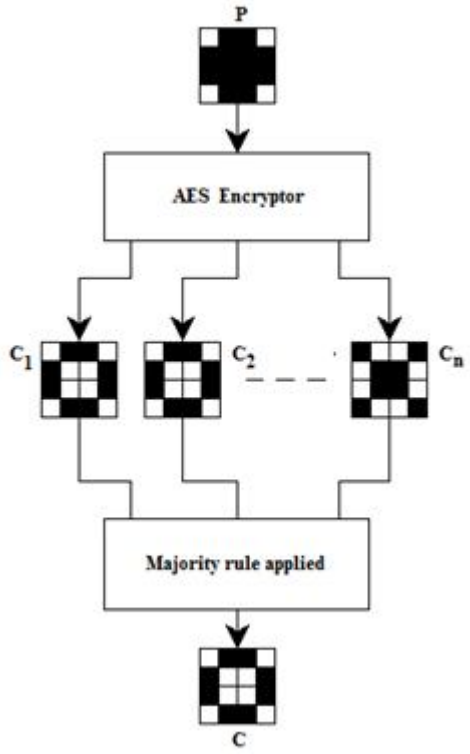

Figure 1. Block Diagram of the proposed scheme

When there is no error injected/generated, the above mentioned plain text is transformed into the following cipher text (Hex values shown) with the above mentioned key:

FC 41 16 48 BE C0 16 A7 FC 5C 3F 43 F4 13 F4 A0

We conduct the experiment where the plain text is encrypted thrice, i.e., the value of n taken in the current experiment is 3 and according to the proposed scheme, not more than one cipher text can be erroneous and two others are quite error free. Now we forcibly inject a one bit error after the first round and as a result the following erroneous cipher text (Hex values shown) is generated:

24 E2 C9 55 1C 30 E0 58 5D D7 3C 64 EA 2F CA F7

Whereas other two ciphers are error free and are as follows (Hex values shown):

FC 41 16 48 BE C0 16 A7 FC 5C 3F 43 F4 13 F4 A0

Now Majority Rule is applied to the three cipher texts listed below:

24 E2 C9 55 1C 30 E0 58 5D D7 3C 64 EA 2F CA F7

FC 41 16 48 BE C0 16 A7 FC 5C 3F 43 F4 13 F4 A0

FC 41 16 48 BE C0 16 A7 FC 5C 3F 43 F4 13 F4 A0

And as a result, the following string is realized:

FC 41 16 48 BE C0 16 A7 FC 5C 3F 43 F4 13 F4 A0

And this is nothing but the error free cipher text.

The parallel architecture of the proposed scheme is shown in Figure 2. Here n numbers of AES Encryptor is used in order to minimize the time of the encryption of the plain text. If t is the time required for a single encryption process, the parallel architecture will take t time for n numbers of encryption processes where as the previous architecture takes n.t time for the same. In addition to the higher speed, the other advantage of the parallel scheme is that the probability of occurrence of errors in all the encryptors at the same time is very less.

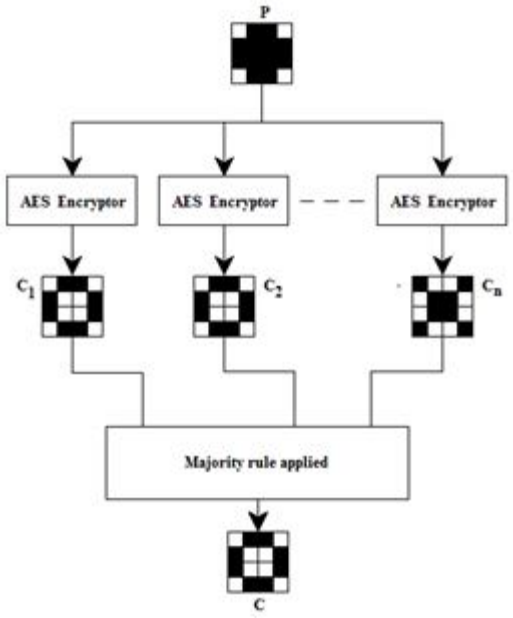

Figure 2. Block Diagram of the parallel architecture

Conclusion

In this paper we have proposed a probabilistic approach towards the prevention of the Error Propagation of Effect. The proposed scheme suggests that n must be odd and the probability of occurrence of a single bit error amidst the rounds of AES encryption must not reach 0.5. That means the number of error free cipher texts is always greater than that of erroneous cipher texts, which ensures that the majority Rule, if applied to the n number of cipher texts generated, will always generate the error free cipher text. It can also be realized that with the increase in the number (n) of cipher texts, the scheme guarantees reliable communication on its part, even with the occurrence of error with higher probability (0.5 * (1 – 1/n)); that means, if n increases the tolerance also increases. Yet a tread off is required. In case of the parallel scheme, since the number of encryptors increases, the hardware complexity increases. Yet the scheme is a superior one.

Reference

[1] NIST, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication, No.197, 26 Nov'2001.

[2] Chandan T Bhunia, "Information Technology, Networks and Internet", New Age International Publishers, New Delhi, 2005.

[3] G. Bertoni, L. Breveglieri, I. Koren, and V. Piuri, "Fault Detection in the Advanced Encryption Standard," Proc. Conf. Massively Parallel Computing Systems (MPCS '02), pp. 92-97, 2002.

[4] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "On the Propagation of Faults and Their Detection in a Hardware Implementation of the Advanced Encryption

DOI: 01.IJNS.3.4.2

Standard," Proc. Int'l Conf. Application-Specific Systems, Architectures, and Processors (ASAP '02), pp. 303-312, 2002.

[5] Guido Bertoni et al. "Error analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard", IEEE Trans on Computers, Vol 52, No 4, pp 492-504, April'2004.

[6] Chandin T Bhunia et al. Project Work on AES Error Propagation, ISM, Deemed University, India, June'2004.

[7] C T Bhunia, New Approaches for Selective AES towards Tackling Error Propagation Effect of AES, Asian J of Information Technology, Pakistan, Vol 5, No. 9, pp 1017-1022, 2006.

[8] Tom Lookabaugh et al, "Selective Encryption for Consumer Applications", IEEE Communication Magazine, Vol 42, no 5, pp.124-129, April, 2004.

DOI: 01.IJNS.3.4.2